

REMARKS

Claims 1-22 are still pending in this application. Reconsideration of the application is earnestly requested. The Examiner has rejected all claims 1-22 under section 103 in view of *Hailpern* and *Trcka*. Although the Examiner's arguments have been carefully considered, Applicant respectfully traverses these rejections as explained below.

The Present Invention

The present invention provides a system and method for the real-time tracking of computer viruses, aggregation of the tracking information, and display of the tracking information. As pointed out in the background of the invention, prior art antivirus systems do not provide any real-time methods for tracking computer virus activity on a distributed network scale (i.e., system wide, nationwide or worldwide). While a user may be able to download antivirus software, "the downloaded antivirus software does not perform any real-time communication of the results back to an antivirus server site to form a collective analysis." (Page three, final paragraph.) It is the lack of such a collective analysis that hampers tracking of a computer virus outbreak and delays preventing further spread of the outbreak. The present invention as claimed provides a solution to such a problem.

As described in the specification, antivirus software running on user's computers worldwide (for example) collects virus data as a result of the scanning of each user's computer. A central server then collects such virus data from each user's computer, consolidates the virus data, and creates virus tracking information that may be viewed on a display by any party. Thus, individual results from many computers are aggregated and a collective analysis is performed to assist with the tracking of a computer virus outbreak. For example, Figure 4B shows the tracking over the past 24 hours for the virus VBS_LOVELETTER-O worldwide; such tracking information is a result of the input from each client computer and the collective analysis performed. The end result is impressive.

The Cited Art Distinguished

U.S. Patent No. 6,275,937 issued to *Hailpern et al.* (*Hailpern*) discusses that one problem with Internet access is that each user must install and run antivirus software on their own computer, and that central processing on the corporate firewall is not desirable (column 3). The

solution provided by *Hailpern* is to provide intermediate proxy servers located within the corporate intranet, but between a client computer and the Internet. These intermediate proxy servers perform the antivirus scanning before data or programs from the Internet arrive at a client computer. Figure 1 shows such a proxy server 1100 located between the Internet 1020 and a client computer 1200. Figure 2 shows a proxy server 1600 located between the corporate firewall 1530 and a client computer 1700. In all cases, the intermediate proxy servers described in *Hailpern* are located within the corporate intranet. Content servers 1000, 1010, 1500 and 1510 are shown for background information and are located remotely and accessible only via the Internet. See column 4, first paragraph, and column 6, lines 24-27.

In other words, the servers referred to and discussed in *Hailpern* are only the intermediate proxy servers located within the corporate intranet. These proxy servers do perform virus scanning (see column 4, first paragraph, lines 39-41; column 5, lines 41-49; column 14, lines 39-42), but the results of a virus scan are not sent to a central location, are not aggregated with other such virus scans, and are not collectively analyzed and displayed for viewing.

Figure 3 of *Hailpern* shows an example of an intermediate proxy server having a virus checking module and a "dangerous source database" that holds results of the virus checking. Each proxy server includes such a database but the virus checking results in each of these databases is not sent to a central location for aggregation, analysis or display. (See column 9, lines 41-51; column 14, lines 39-42; column 16, lines 51-55.)

By contrast, the present invention as claimed requires that each client computer generate a scan log, that each scan log be sent to a virus tracking server, that the collective scan log information be processed into virus tracking information, and that the resultant virus tracking information be displayed on a user device.

Claim 12 specifically requires "sending the scan log back from each client user," "receiving the scan log from said client computers in real-time via a virus tracking server," and "processing the scan log information into virus tracking information." Claim 1 specifically requires "a scan log which is sent back from each client user," "a virus tracking server for receiving the scan log information from said client computers in real-time," and "processing the scan log information into virus tracking information." *Hailpern* does not teach or suggest these steps because the results of virus checking on a *Hailpern* proxy server are not sent back

anywhere, are not received at a central virus tracking server and are not processed into valuable virus tracking information.

For these reasons, it is respectfully noted that there is no prima facie case of obviousness, and it is requested that the rejection of claims 1-22 be withdrawn.

Claims 11 and 22

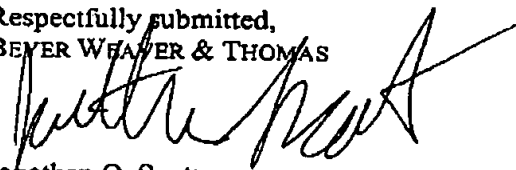
Since claims 11 and 22 depend on the independent claims, it is respectfully submitted that they are each patentable over the art of record for at least the same reasons as set forth above with respect to claims 1 and 12. Further, each of these dependent claims require additional features that when considered in light of the claimed combination further distinguish the claimed invention from the art of record. Claims 11 and 22 have been amended to clarify that when the distributed computer network includes the Internet that each client computer sends its scan log back over the Internet to the central virus tracking server. Thus, information available from virtually any client computer worldwide can be aggregated and analyzed on a central server located almost anywhere. Indeed, the specification points out that "the Internet provides an ideal medium for such tracking since it is distributed, fast, and can provide real-time feedback," (page 15, first paragraph). Claim 11 further requires that the display mode is accessible over the Internet, and claim 22 requires that the real-time trace is made available over the Internet.

By contrast, *Hailpern* does not disclose that the results of virus checking performed on an intermediate proxy server are sent anywhere, let alone back over an Internet connection to a central server. *Hailpern* discloses clearly (as shown in Figures 1 and 2) that the proxy servers performing the virus checking are located within the same corporate intranet as the client computers; thus, no benefit can be obtained because the results of disparate client computers (perhaps located on many different corporate intranets) cannot be aggregated on a central server accessible over an Internet connection. For these reasons, it is submitted that dependent claims 11 and 22 are patentable and it is requested that the rejection be withdrawn.

Reconsideration of this application and issuance of a Notice of Allowance at an early date are respectfully requested. If the Examiner believes a telephone conference would in any way

expedite prosecution, please do not hesitate to telephone the undersigned at (612) 252-3330.

Respectfully submitted,
BEYER WEAVER & THOMAS



Jonathan O. Scott
Registration No. 39,364

BEYER WEAVER & THOMAS, LLP
P.O. Box 778
Berkeley, CA 94704-0778

Telephone: (612) 252-3330
Facsimile: (612) 825-6304